

COURSE OVERVIEW

Course Name:
(CS0-002)
CompTIA Cybersecurity Analyst CySA+

COURSE DURATION: 5 Day

Gauteng:

3rd Floor, 34 Whitely Road
Melrose Arch
Johannesburg
2196

Gauteng:

192 on Bram
192 Bram Fischer Drive
Ferndale, Randburg
Johannesburg
2160

Cape Town:


3rd Floor, Thomas Pattullo Building
19 Jan Smuts St
Cape Town
8000

Durban:

9 Mountview Close
Broadlands
Mount Edgecombe
Durban
4302

 **087 941 5764**

 **sales@impactful.co.za**

 **impactful.co.za**

INTRODUCTION

The CompTIA Cybersecurity Analyst (CySA+) course is an international, vendor-neutral cybersecurity certification that applies behavioural analytics to improve the overall state of IT security. The CySA+ course validates knowledge and skills that are required to prevent, detect, and combat cybersecurity threats.

In addition, this course covers the duties of those who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. Depending on the size of the organization, this individual may act alone or may be a member of a cybersecurity incident response team (CSIRT).

The course introduces delegates to tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect, and analyse cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed towards those on the front lines of defence.

DELIVERY METHOD

Our courses have flexible delivery options:

- In-person classroom training at the Impactful training facilities
 - Johannesburg, Durban, Cape Town
- Virtual instructor-led training
- Nationally: on-site at the client

INTENDED AUDIENCE

This course is designed primarily for cybersecurity practitioners who perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

This course focuses on the knowledge, ability, and skills necessary to provide for the defence of those information systems in a cybersecurity context, including protection, detection, analysis, investigation, and response processes.

In addition, the course ensures that all members of an IT team—everyone from help desk staff to the Chief Information Officer—understand their role in these security processes.

PREREQUISITES

Before attending this course, delegates must have achieved the following requirements:

- At least two years (recommended) of experience in computer network security technology or a related field
- The ability to recognize information security vulnerabilities and threats in the context of risk management
- Foundation-level operational skills with some of the common operating systems for computing environments
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms
- Foundation-level understanding of some of the common concepts for network environments, such as routing and switching
- Foundational knowledge of major TCP/IP networking protocols, including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.

You can obtain this level of skills and knowledge by taking the following courses:

CompTIA A+ Bootcamp;
CompTIA Network+ course;

COURSE OBJECTIVES

After completing the CompTIA CySA+ course, delegates will have the skills and knowledge to:

- Assess information security risk in computing and network environments
- Analyse the cybersecurity threat landscape
- Analyse reconnaissance threats to computing and network environments
- Analyse attacks on computing and network environments
- Analyse post-attack techniques on computing and network environments
- Implement a vulnerability management program
- Evaluate the organization's security through penetration testing
- Collect cybersecurity intelligence
- Analyse data collected from security and event logs
- Perform active analysis on assets and networks
- Respond to cybersecurity incidents
- Investigate cybersecurity incidents
- Address security issues with the organization's technology architecture

COURSE CONTENT

Lesson 1: Assessing Information Security Risk

Lesson 2: Analysing the Threat Landscape

Lesson 3: Analysing Reconnaissance Threats to Computing and Network Environments

Lesson 4: Analysing Attacks on Computing and Network Environments

Lesson 5: Analysing Post-Attack Techniques

Lesson 6: Managing Vulnerabilities in the Organization

Lesson 7: Implementing Penetration Testing to Evaluate Security

Lesson 8: Collecting Cybersecurity Intelligence

Lesson 9: Analysing Log Data

Lesson 10: Performing Active Asset and Network Analysis

Lesson 11: Responding to Cybersecurity Incidents

Lesson 12: Investigating Cybersecurity Incidents

Lesson 13: Addressing Security Architecture Issues

ASSOCIATED CERTIFICATION AND EXAM

This course is designed to prepare the students to take the CompTIA CS0-002 international examination. Successfully passing this exam will result in the attainment of the CompTIA Cybersecurity Analyst (CySA+) certification.